COMITATO NAZIONALE PER L'ENERGIA NUCLEARE
Laboratori Nazionali di Frascati

LNF - 70/63
Dicembre 1970

(Lezioni)

G. Tallini e E.G. Beltrametti: GEOMETRIE DI GALOIS E LORO APPLICAZIONI ALLA FISICA. -

Servizio Documentazione
dei Laboratori Nazionali di Frascati del CNEN
Casella Postale 70 - Frascati (Roma)

LNF-70/63

G. Tallini e E. G. Beltrametti

GEOMETRIE DI GALOIS E LORO APPLICAZIONI ALLA FISICA

Seminari tenuti nei
Laboratori Nazionali del CNEN
Frascati, 1970

I. - INTRODUZIONE ALLE GEOMETRIE DI GALOIS. -

(A cura di G. Tallini, Università di Napoli)

Simboli usati

$\in$	"è un elemento di"
$\notin$	"non è un elemento di"
$\forall$	"per ogni"
$\exists$	"esiste"
$:$	"tale che"
$\Longrightarrow$	"implica"
$\Longleftrightarrow$	"equivale"

I.1. - Campi di Galois. -

Chiamasi campo un insieme K munito di una operazione di somma (+) ed una operazione di prodotto ($\cdot$) in modo che siano soddisfatte le proprietà seguenti:

1) $\forall\, a,b,c \in K \Longrightarrow (a+b)+c = a+(b+c)$, proprietà associativa di +;

2) $\forall\, a,b \in K \Longrightarrow a+b = b+a$, proprietà commutativa di +;

3) $\exists\, 0 \in K : \forall\, a \in K \Longrightarrow 0+a = a$, esistenza dell'elemento neutro rispetto a +;

4) $\forall\, a \in K \Longrightarrow \exists\, (-a) \in K : a+(-a) = 0$, esistenza dell'opposto;

1') $\forall\, a,b,c \in K \Longrightarrow (ab)c = a(bc)$, proprietà associativa di $\cdot$;

2') $\forall\, a,b \in K \Longrightarrow ab = ba$, proprietà commutativa di $\cdot$;

3') $\exists\, 1 \in K : \forall\, a \in K \Longrightarrow 1 \cdot a = a$, esistenza dell'elemento neutro rispetto a $\cdot$;

4') $\forall\, a \in K - \{0\} \Longrightarrow \exists\, a^{-1} \in K : aa^{-1} = 1$, esistenza dell'inverso;

5) $\forall\, a,b,c \in K \Longrightarrow a(b+c) = ab + ac$, proprietà distributiva.

L'insieme Q dei numeri razionali, l'insieme R dei reali, l'insieme $\mathbb{C}$ dei complessi, rispetto alle usuali operazioni di somma e di prodotto, costituiscono altrettanti esempi di campi. L'insieme Z degli interi relativi, rispetto alle usuali operazioni di somma e di prodotto, non costituisce invece un campo in quanto per esso (pur valendo tutte le proprietà 1, 2, 3, 4, 1', 2', 3', 5) non vale la proprietà 4'. Più in generale definisce si anello (commutativo unitario) un insieme K munito di una operazione di somma ed una di prodotto in modo che siano soddisfatte le proprietà 1, 2, 3, 4, 1', 2', 3', 5. Dunque $(Z, +, \cdot)$ è un anello: l'anello degli interi relativi. Diremo che due campi (o anelli) K e K' sono isomorfi se esiste tra essi una corrispondenza biunivoca $\varphi : K \to K'$ che conserva le operazioni (cioè tale che $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(a,b) = \varphi(a) \cdot \varphi(b)$, per ogni a, b di K). In sostanza due campi (o anelli) isomorfi differiscono solamente per la natura degli oggetti che li compongono, ma non per la struttura algebrica in essi definita, perciò essi possono pensarsi identificati, mediante φ.

In un campo K valgono tutte le proprietà usuali (che seguono dalle 1-4, 1'-4', 5) valide per esempio nel campo reale. Si può parlare di equazione algebrica a coefficienti in K, radice di una tale equazione, elemento quadrato o non quadrato in K, radice quadrata di un elemento quadrato di K, forma quadratica in più variabili, sostituzioni lineari, matrici, determinanti, ecc. Per esempio in un campo K vale la ben nota legge di annullamento di un prodotto:

$$(1.1) \qquad a, b \in K, \quad ab = 0 \iff a = 0 \quad \text{oppure} \quad b = 0$$

(Infatti dalla proprietà distributiva della differenza $a(b-c) = ab - ac$, che segue facilmente dalle proprietà che definiscono un campo, si ha, per $b=c$, $a0 = 0a = 0$. Viceversa, se $ab = 0$ ed è $a \neq 0$, esistendo in K l'inverso a^{-1} di a, si ottiene $a^{-1}(ab) = 0$ da cui $b = 0$). Osserviamo che in un anello A vale, nella (1.1), la freccia $\Longleftarrow$ ma non la freccia $\Longrightarrow$; possono cioè esistere in A elementi a, b, ambedue diversi da zero, tali che $ab = 0$. Siffatti elementi prendono il nome di divisori dello zero di A. Daremo nel seguito esempi di anelli dotati di divisori dello zero.

Nasce naturale la questione di indagare se esistono campi finiti, cioè campi con un numero finito di elementi (ordine del campo). Ci occuperemo ora di questo problema.

Sia p un fissato intero ≥ 2. Per ogni intero h, con $0 \leq h \leq p-1$, denoteremo con $[h]$ la classe degli interi relativi che divisi per p danno come resto h, cioè la classe degli interi $\{np+h\}_{n \in Z}$. Si ottengono in tal modo esattamente p classi:

$$(1.2) \qquad [0], [1], [2], \ldots, [p-1]$$

a due a due prive di elementi in comune e tali che ogni intero relativo appartiene ad una sola di tali classi (Per esempio, per $p = 2$, si ottengono la classe $[0]$, costituita dagli interi pari, e la classe $[1]$, costituita dagli interi dispari). Esse prendono il nome di classi dei resti mod p. Ciascuna di esse può essere individuata da un qualsiasi intero in essa contenuto, quindi scriveremo anche $[h] = [h+np]$. Cosi risulta $[0] = [p]$, $[p-1] = [-1]$, $[p-2] = [-2]$, ecc.

Osserviamo che, qualsiasi siano le classi $[h]$, $[k]$, la somma o il prodotto di un qualunque intero di $[h]$ per un qualunque intero di $[k]$ è un intero della classe $[h+k]$ o $[hk]$. Possiamo allora porre, senza alcuna ambiguità:

$$(1.3) \qquad [h] + [k] = [h+k],$$

$$(1.4) \qquad [h] \cdot [k] = [hk].$$

Rispetto a tali operazioni di somma e di prodotto, l'insieme delle classi dei resti mod p costituisce - come subito si prova - un anello (commutativo unitario) nel senso che sono verificate le proprietà 1-4, 1'-3', 5. Tale anello prende il nome di anello delle classi dei resti mod p e verrà denotato con Z_p. Esso è un anello finito di ordine p. Lo zero di Z_p è $0 = [0]$ e l'unità di Z_p è $1 = [1]$.

Se p non è primo, cioè $p = hk$, con $1 < h < p$, $1 < k < p$, in Z_p si ha, per la (1.4), $[h][k] = [p] = [0] = 0$ con $[h] \neq 0$, $[k] \neq 0$. Dunque Z_p possiede divisori dello zero, onde Z_p non è un campo, anzi Z_p dà un esempio di anello con divisori dello zero.

Supponiamo ora che p sia primo e proviamo che Z_p è un campo, cioè che vale la 4', ossia che per ogni $[h] \neq 0$ esiste un $[k] \in Z_p$ tale che $[h][k] = 1$. Poichè

p è il primo, Z_p non ha divisori dello zero (infatti da $[h]\,[k] = 0$ segue che $[hk] = 0$ e quindi che hk è divisibile per p; ma p è primo, onde o h è divisibile per p, ossia $[h] = 0$, oppure k è divisibile per p, ossia $[k] = 0$). Si consideri l'applicazione $\varphi: [k] \in Z_p - \{0\} \longrightarrow [h]\,[x] \in Z_p - \{0\}$, essa è iniettiva (in quanto, se fosse $[h]\,[x] = [k]\,[x]$, si avrebbe $([h] - [k])\,[x] = 0$, e quindi, poichè Z_p non ha divisori dello zero ed è $[x] \neq 0$, si otterebbe $[h] - [k] = 0$, cioè $[h] = [k]$). Poichè $Z_p - \{0\}$ è finito, la φ deve essere biunivoca, dunque al variare di $[x]$ in $Z_p - \{0\}$, $[h]\,[x]$ descrive tutti gli elementi di $Z_p - \{0\}$. Esisterà dunque un ben determinato $\{\bar{x}\}$ tale che $[h]\,[\bar{x}] = 1$. Abbiamo così provato che

a) L'anello Z_p è un campo se, e soltanto se, p è primo.

Sia p un primo, il campo Z_p prende anche il nome di campo fondamentale d'ordine p. Supponiamo che in Z_p l'equazione $x^2 + 1 = 0$ non ammetta soluzioni (come accade per esempio per $p = 3, 7, 11, 19, 23$, e più in generale per tutti i primi p tali che $p \equiv -1 \bmod 4$). Si introduca un simbolo $\underline{i}$ soggetto alla condizione che sia $\underline{i}^2 = -1$ e si considerino i polinomi di primo grado in $\underline{i}$ a coefficienti in Z_p, cioè gli elementi $a + \underline{i}b$, con $a, b \in Z_p$. Operando per somma e prodotto nel modo usuale tra tali elementi e tenendo conto che $\underline{i}^2 = -1$, si perviene -come subito si prova - ad un campo, ottenuto in sostanza proprio come può farsi per passare dal campo dei numeri reali a quello dei numeri complessi. Il campo così ottenuto è finito ed è costituito da p^2 elementi (in quanto essi si ottengono, e ciascuno una volta sola, facendo assumere in $\underline{a} + \underline{i}\underline{b}$, ad $\underline{a}$ i p valori distinti di Z_p e così dicasi per $\underline{b}$). Tale campo sarà denotato con $GF(p^2)$ (o più semplicemente con G_{p2}) e prende il nome di ampliamento algebrico di grado 2 di Z_p o di campo di Galois d'ordine p^2.

Il procedimento suesposto può generalizzarsi nel modo seguente. Sia

$$g(x) = x^h + g_1 x^{h-1} + g_2 x^{h-2} + \ldots + g_{n-1} x + g_n, \qquad g_s \in Z_p \tag{1.5}$$

un polinomio di grado $h \geq 2$, a coefficiente in Z_p (p primo) ed ivi irriducibile (ossia che non si possa scomporre in fattori propri a coefficienti in Z_p). Si introduce un simbolo $\underline{i}$ (immaginario di Galois) soggetto alla condizione che sia $g(\underline{i}) = 0$, cioè:

$$\underline{i}^h = -(g_1 \underline{i}^{h-1} + g_2 \underline{i}^{h-2} + \ldots + g_{h-1} \underline{i} + g_h). \tag{1.6}$$

Si considerino i polinomi di grado $h - 1$ in $\underline{i}$ a coefficienti in Z_p, cioè gli elementi:

$$\underline{a}_1 \underline{i}^{h-1} + \underline{a}_2 \underline{i}^{h-2} + \ldots + \underline{a}_{h-1} \underline{i} + \underline{a}_h, \qquad a_s \in Z_p \tag{1.7}$$

Operando per somma e per prodotto nel modo usuale tra tali elementi e tenendo conto della (1.6) si perviene - come si può provare - ad un campo. Esso è finito ed è costituito da p^h elementi (in quanto essi si ottengono, e ciascuno una volta sola, facendo assumere nella (1.7) a ciascuno degli a_s i p valori distinti di Z_p). Tale campo prende il nome di ampliamento algebrico di grado h di Z_p relativo al polinomio (1.5) o di campo di Galois d'ordine p^h. Si può dimostrare che, se si parte da due polinomi diversi, ambedue di grado h, a coefficienti in Z_p ed ivi irriducibili, i due campi di Galois ottenuti nel modo anzidetto da essi risultano isomorfi. Dunque esiste un solo campo di Galois d'ordine p^h a meno d'isomorfismi. Un tale campo sarà denotato con $GF(p^h)$ o più semplicemente con G_{ph}; il primo p sarà detto caratteristica del campo di Galois. Il campo Z_p sarà anche denotato con GF(p) o G_p e si dirà anche campo di Galois d'ordine p.

Ci si può chiedere se esistono altri campi finiti, oltre ad i campi di Galois. La risposta è negativa, sussistono anzi i seguenti fondamentali teoremi sui campi finiti:

b) Ogni campo finito è isomorfo ad un campo di Galois ed ha quindi ordine $q = p^h$.

c) Fissati comunque un primo p ed un intero positivo h, esiste uno ed un sol campo di Galois d'ordine $q = p^h$, a meno d'isomorfismi.

I. 2. - Quadrati e non quadrati in un campo di Galois Gq. Forme quadratiche su Gq. -

Sia Gq un campo di Galois d'ordine q. Denoteremo con G_q' l'insieme dei q-1 elementi non nulli di G_q. Un elemento di G_q si dirà quadrato se esiste un x in G_q tale che $y = x^2$, in caso contrario si dirà che y è un non quadrato. Denoteremo con $\square$ l'insieme dei quadrati di G_q, con $\square'$ l'insieme dei quadrati non nulli e con $\not\square$ l'insieme dei non quadrati di G_q. Ci occuperemo ora dello studio degli elementi quadrati e non quadrati di G_q.

Supponiamo per primo che q sia pari, cioè $q = 2^h$. In tal caso, essendo $2 = 0$, risulta $1 = -1$. L'applicazione $\sigma : x \in G_q \to x^2 \in G_q$ è allora iniettiva (cioè elementi distinti vanno in elementi distinti: infatti, se $x^2 = y^2$, risulta $x = \pm y$ e quindi $x = y$, in quanto $\pm 1 = 1$); poichè G_q è finito, σ risulta dunque biunivoca. Ne segue che:

d) In un campo di Galois G_q, con q pari ($q = 2^h$), ogni elemento è un quadrato.

Supponiamo ora che q sia dispari, cioè $q = p^h$ con p primo e $p > 2$. I q-1 elementi non nulli di G_q si possono distribuire in (q-1)/2 coppie, ciascuna costituita da elementi tra loro opposti (e quindi diversi tra loro perchè $1 \neq -1$). Ogni quadrato non nullo di G_q è il quadrato di due elementi non nulli tra loro opposti. Dunque vi è corrispondenza biunivoca tra gli elementi quadrati non nulli di G_q e le (q-1)/2 coppie suddette. Ne segue che i quadrati non nulli di G_q sono in numero di (q-1)/2 e quindi i non quadrati sono anche in numero di (q-1)/2 (in quanto q-1 sono gli elementi non nulli di G_q).

Osserviamo che evidentemente il prodotto di due quadrati è un quadrato e così il prodotto di un quadrato per un non quadrato è un non quadrato. Proviamo che il prodotto di due non quadrati è un quadrato: sia a un non quadrato di G_q, si consideri l'applicazione $\tau : x \in G_q' \to ax \in G_q'$; essa è biunivoca, inoltre, per quanto precede, se x è un quadrato non nullo di G_q, ax è un non quadrato di G_q; dunque quando x descrive $\square'$, l'elemento ax descrive tutto $\not\square$; ne segue che quando x descrive $\not\square$, l'elemento ax descrive tutto $\square'$; onde l'asserto. Si è così provato che:

e) In un campo di Galois G_q, con q dispari, il numero degli elementi non quadrati uguaglia quello degli elementi quadrati non nulli ed è dato da (q-1)/2. Inoltre sussiste la seguente regola per il prodotto:

$$\begin{aligned} \square \cdot \square &= \square \\ \square \cdot \not\square &= \not\square \cdot \square = \not\square \\ \not\square \cdot \not\square &= \square \end{aligned} \qquad (2.1)$$

Osserviamo che nel campo dei numeri reali R i numeri positivi coincidono con i quadrati non nulli e i negativi con i non quadrati di R e che in R vale una regola

del prodotto del tutto analoga alla (2.1). Dunque gli elementi quadrati e non quadrati di G_q si comportano moltiplicativamente come i reali positivi e quelli negativi rispettivamente. Però non sussiste l'analogo additivamente: la somma di due quadrati di G_q può essere un non quadrato di G_q (a differenza di quanto accade nel caso reale). Sussiste anzi la seguente proposizione:

f) Dato comunque un elemento non quadrato k di G_q (q dispari), esistono sempre in G_q due quadrati, x^2 ed y^2, tali che $x^2 + y^2 = k$.

Dimostrazione. Ragionando per assurdo supponiamo che l'equazione $x^2 + y^2 = k$, nelle incognite x, y, non ammetta nessuna soluzione in G_q. In tale ipotesi allora, qualsia si sia x in G_q, l'elemento $k - x^2$ è un non quadrato di G_q. D'altra parte, al variare di x in G_q, $k - x^2$ assume $[(q-1)/2+1]$ valori tutti distinti di G_q (tanti quanti sono i quadrati di G_q), i quali dovrebbero essere tutti non quadrati di G_q. Ma ciò è assurdo perchè i non quadrati di G_q sono solamente $(q-1)/2$. Si ha cosi l'asserto.

Dalla prop. f) si ha per esempio che l'equazione $x^2 + y^2 + 1 = 0$ ammette sempre soluzione in G_q (q dispari), a differenza di quanto accade nel caso reale.

La proposizione f) ammette la seguente generalizzazione:

g) Sia $f(x_1, x_2, \ldots, x_n)$ una qualsivoglia forma quadratica, nelle indeterminate $x_1, x_2, \ldots, x_n$, a coefficienti in Gq (q dispari), che non risulti il quadrato di una forma lineare. Scelto comunque un elemento h di G_q esiste almeno una n-pla di elementi di G_q, $(\mathring{x}_1, \mathring{x}_2, \ldots, \mathring{x}_n)$, tale che $f(\mathring{x}_1, \mathring{x}_2, \ldots, \mathring{x}_n) = h$.

Dimostrazione. Non è restrittivo supporre che la f sia ridotta a forma diagonale, cioè:

$$(2.2) \qquad f = a_1x_1^2 + a_2x_2^2 + \ldots + a_mx_m^2, \qquad a_s \in G_q', \qquad 2 \leq m \leq n$$

in quanto a meno di una sostituzione lineare invertibile a coefficienti in G_q nelle indeterminate, ci si può sempre ridurre alla (2.2) (basta procedere in modo del tutto analogo al caso reale). L'equazione $[(a_1/a_2)x^2] + y^2 = h/a_2$ ammette sempre almeno una soluzione (x_o, y_o) in G_q (basta procedere come nella dimostrazione della proposizione f)), onde $a_1x_o^2 + a_2y_o^2 = h$ e quindi la n-pla $(x_o, y_o, 0, 0, \ldots, 0)$ di elementi di G_q fa assumere ad f il valore h. Onde l'asserto.

Osserviamo che se, con analogia al caso reale, si definiscono "positivi" i quadrati non nulli e "negativi" i non quadrati di G_q, non esistono forme quadratiche definite "positive" o definite "negative" in G_q, ciò in forza della prop. g).

Un corollario della prop. g) è la seguente proposizione:

h) Sia $f(x_1, x_2, \ldots, x_n)$, $n \geq 3$, una qualsivoglia forma quadratica a coefficienti in G_q (q dispari). Esiste sempre qualche n-pla di elementi non tutti nulli di G_q $(\mathring{x}_1, \mathring{x}_2, \ldots, \mathring{x}_n)$ tale che $f(\mathring{x}_1, \mathring{x}_2, \ldots, \mathring{x}_n) = 0$.

Dimostrazione. Non è restrittivo supporre che la f sia non degenere (cioè abbia il determinante della matrice dei coefficienti diverso da zero). Riducendo la f a forma diagonale si ha:

$$(2.3) \qquad f = a_1x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2, \qquad a_s \in G_q' .$$

Basta evidentemente provare l'asserto per la (2. 3). Si consideri la forma quadratica $g(x_1, x_2) = a_1x_1^2 + a_2x_2^2$. Essa non è evidentemente il quadrato di una forma lineare. Per la prop. g) allora esiste una coppia $(\mathring{x}_1, \mathring{x}_2)$ di elementi di G_q tale che $a_1\mathring{x}_1 + a_2\mathring{x}_2 = -a_3$. La n-pla non tutta nulla $(\mathring{x}_1, \mathring{x}_2, 1, 0, \ldots, 0)$ di elementi di G_q annulla dunque il secondo membro della (2. 3). Si ha così l'asserto.

I. 3. - Piano affine su un campo di Galois G_q.

Denoteremo con π_q l'insieme delle coppie di elementi di un campo di Galois G_q (cioè si pone $\pi_q = G_q \times G_q$). Un elemento di π_q (cioè una coppia (x, y) con $x \in G_q$, $y \in G_q$) sarà detto punto di π_q. Chiameremo retta di π_q l'insieme dei punti (x, y) di π_q che soddisfano una equazione lineare $ax + by + c = 0$. Sia R l'insieme delle rette di π_q. La coppia (π_q, R) prende il nome di piano affine su G_q. Esso sarà sovente denotato semplicemente con π_q. Due rette di π_q si direnno parallele se non hanno alcun punto in comune o coincidono, cioè se i coefficienti (a, b) e (a', b') di x ed y nelle loro equazioni sono proporzionali ($a' = ka$, $b' = kb$, $k \leq G_q$). In π_q si può sviluppare la geometria analitica affine in modo analogo a quanto si fa nel caso reale. Si prova per esempio subito che:

1) Per due punti distinti di π_q passa una ed una sola retta.
2) Per un punto P di π_q passa una sola retta parallela ad una retta data.

Se K è un insieme finito, denoteremo con $|K|$ il numero degli elementi di K. Ciò premesso, si dimostra facilmente la seguente proporzione:

i) Sia π_q un piano affine su G_q. Denotati con r una qualsiasi retta di π_q, F_r l'insieme delle rette parallele ad r (fascio improprio di rette determinato da r o direzione di r), F_P l'insieme delle rette per un qualsiasi punto P di π_q (fascio di rette di centro P), R l'insieme delle rette di π_q, risulta:

$$|\pi_q| = q^2, \quad |r| = q, \quad |F_r| = q, \quad |F_P| = q+1, \quad |R| = q^2+q. \tag{3.1}$$

Chiamasi affinità di π_q la corrispondenza biunivoca $\alpha : (x, y) \in \pi_q \to (x', y') \in \pi_q$ tra i punti di π_q di equazioni:

$$x' = a_{11}x + a_{12}y + a_1 ; \qquad y' = a_{21}x + a_{22}y + a_2 \tag{3.2}$$

ove è:

$$a_{ij} \in G_q, \quad a_i \in G_q, \quad a_{11}a_{22} - a_{12}a_{21} \neq 0 . \tag{3.3}$$

Evidentemente una affinità di π_q muta rette in rette e coppie di rette parallele in coppie di rette parallele.

L'insieme delle affinità di π_q, rispetto al prodotto operatorio, costituisce un gruppo che sarà denotato con A_q. Definiscesi geometria affine lo studio delle proprietà delle figure di π_q invarianti rispetto al gruppo A_q. Nella geometria affine di π_q dunque due figure si considerano uguali se esiste una affinità che muta l'una nell'altra. La nozione di parallelismo tra rette è quindi una nozione affine (perchè il parallelismo si conserva per affinità), così la nozione di parallelograma. Proviamo che:

k) Le affinità di π_q sono in numero di $q^3(q-1)^2(q+1)^2$, cioè:

$$|A_q| = q^3(q-1)^2(q+1). \tag{3.4}$$

Dimostrazione. Ogni affinità (3.2) determina la coppia di rette di π_q:

$$a_{11}x + a_{12}y + a_1 = 0\ ; \qquad a_{21}x + a_{22}y + a_2 = 0 \tag{3.5}$$

le quali non sono parallele, in virtù della $(3.3)_{III}$. Viceversa ogni coppia di rette non parallele di π_q di equazioni (3.5) determina le $(q-1)^2$ affinità:

$$x' = h(a_{11}x + a_{12}y + a_1)\ ; \qquad y' = k(a_{21}x + a_{22}y + a_2)$$

ottenute al variare comunque di h e k in G_q' (e si noti che $|G_q'| = q-1$). Dunque $|A_q|$ è dato dal prodotto di $(q-1)^2$ per il numero N delle coppie di rette non parallele di π_q. Determiniamo N. Fissata una retta r di π_q, le rette non parallele ad r sono in numero di q^2 (infatti tutte le rette di π_q sono in numero di q^2+q e tra esse esattamente q sono parallele ad r); poichè r può fissarsi in q^2+q modi si ha: $N = q^2(q^2+q)$. Ne segue che è:

$$|A_q| = (q-1)^2 N = (q-1)^2 q^2 (q^2+q),$$

cioè la (3.4). Onde l'asserto.

Siano $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, $P_3(x_3, y_3)$ tre punti distinti ed allineati di π_q. Se la retta r che li congiunge non è parallela nè all'asse x nè all'asse y, si prova subito che è:

$$\frac{x_2 - x_1}{x_3 - x_1} = \frac{y_2 - y_1}{y_3 - y_1} \in G_q$$

Ciò premesso, definiscesi rapporto semplice P_1P_2/P_1P_3 della terna di punti (P_1, P_2, P_3), col porre:

$$\frac{P_1P_2}{P_1P_3} = \frac{x_2 - x_1}{x_3 - x_1} = \frac{y_2 - y_1}{y_3 - y_1}\ . \tag{3.6}$$

Se la retta r congiungente i tre punti è parallela all'asse x oppure all'asse y, il rapporto semplice di (P_1, P_2, P_3) lo si definisce ponendo rispettivamente:

$$\frac{P_1P_2}{P_1P_3} = \frac{x_2 - x_1}{x_3 - x_1}\ , \qquad \frac{P_1P_2}{P_1P_3} = \frac{y_2 - y_1}{y_3 - y_1}\ . \tag{3.7}$$

E' facile provare che il rapporto semplice P_1P_2/P_1P_3 è invariante per affinità, cioè è un invariante affine della terna (P_1, P_2, P_3).

Si prova facilmente il teorema di Talete:

1) Se r ed r' sono due rette di π_q ed s_1, s_2, s_3 sono tre rette parallele distinte di π_q, che non siano parallele nè ad r nè ad r', denotati con P_1, P_2, P_3 i punti d'incontro di r con s_1, s_2, s_3 e con P_1', P_2', P_3' i punti d'incontro di r' con s_1', s_2', s_3' risulta:

$$P_1P_2/P_1P_3 = P_1'P_2'/P_1'P_3'\ .$$

Se q è dispari ed è $P_1P_2/P_1P_3 = 1/2$, si dice che P_2 è punto medio tra P_1 e P_3. Si prova subito che allora è:

$$x_2 = \frac{x_1 + x_3}{2}, \qquad y_2 = \frac{y_1 + y_3}{2}. \tag{3.8}$$

Sempre nell'ipotesi che sia q dispari si definisce simmetria di centro un punto $P_o(x_o, y_o)$ di π_q la corrispondeza biunivoca di π_q che fa corrispondere ad un punto $P(x, y)$ di π_q il punto $P'(x', y')$ simmetrico di P rispetto a P_o (cioè il punto P' della retta PP_o tale che P_o sia punto medio tra P e P'). Essa ha equazioni:

$$x' = 2x_o - x, \qquad y' = 2y_o - y \tag{3.9}$$

ed è quindi una affinità.

In modo del tutto analogo al caso reale si definisce la simmetria (obliqua) con asse una retta a di π_q e avente una data direzione d non parallela ad a (cioè la corrispondenza biunivoca tra i punti di π_q che fa corrispondere, ad ogni punto P di π_q, il punto P' appartenente alla retta r per P parallela a d e tale che il punto intersezione di r con a sia punto medio tra P e P'). Si determinano facilmente le equazioni di una tale simmetria e si costata che essa è una affinità.

I.4. - Piano euclideo su un campo di Galois G_q, con q dispari. -

Sia θ un fissato elemento non quadrato di un campo di Galois G_q, q dispari. Per ogni a di G_q porremo:

$$|a| = \begin{cases} a, & \text{se } a \in \square \\ \theta a, & \text{se } a \in \not\square \end{cases} \tag{4.1}$$

Poichè il prodotto di due non quadrati di G_q è un quadrato di G_q si ha:

$$\forall a \in G_q, \qquad |a| \in \square \tag{4.2}$$

Osserviamo che, essendo $\theta \in \not\square$, la forma quadratica

$$\nu = x^2 - \theta y^2 \tag{4.3}$$

si annulla se, e soltanto se, risulta $x = y = 0$ (infatti se fosse $x^2 - \theta y^2 = 0$ ed $y \neq 0$, si avrebbe $\theta = x^2/y^2$ cioè $\theta \in \square$, contro il supposto).

Chiamasi piano euclideo su G_q la coppia costituita dal piano affine π_q su G_q e dalla applicazione:

$$N : (P_1, P_2) \in \pi_q \times \pi_q \to N(P_1, P_2) \in G_q \tag{4.4}$$

definita da:

$$N(P_1, P_2) = (x_1 - x_2)^2 - \theta (y_1 - y_2)^2, \qquad P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2). \tag{4.5}$$

Un piano euclideo su G_q lo si continuerà a denotare con π_q. L'elemento $N(P_1, P_2)$ di G_q prende il nome di norma dei punti P_1, P_2. Dall'osservazione precedente si ha:

$$N(P_1, P_2) = 0 \iff P_1 = P_2. \tag{4.6}$$

Inoltre risulta:

$$N(P_1, P_2) = N(P_2, P_1). \tag{4.7}$$

Essendo, per la (4.2), $|N(P_1, P_2)| \in \square$ si può definire la distanza dei punti P_1, P_2 con il porre:

$$d(P_1, P_2) = \pm\sqrt{|N(P_1, P_2)|}\ . \tag{4.8}$$

Essa è determinata a meno del segno.

Due rette $ax+by+c=0$ ed $a'x+b'y+c'=0$ si dicono ortogonali se risulta:

$$\theta\, a a' - b b' = 0. \tag{4.9}$$

Dall'osservazione precedente segue che due rette ortogonali non possono mai essere parallele cioè sono sempre incidenti. Si ha poi che per un punto $P_0(x_0, y_0)$ passa una sola retta ortogonale ad una data retta $ax+by+c=0$, precisamente la retta di equazione:

$$b(x - x_0) + \theta\, a(y - y_0) = 0\ . \tag{4.10}$$

Ne segue che le rette ortogonali ad una data retta r costituiscono un fascio di rette parallele, cioè una direzione, che dicesi ortogonale ad r. Tale direzione è poi ortogonale ad ogni retta parallela ad r. Si può dunque parlare di direzioni ortogonali. Inoltre la nozione di ortogonalità tra rette è involutaria nel senso che se r è ortogonale ad r' allora r' è ortogonale ad r.

La definizione data di ortogonalità è giustificata dalla validità del seguente teorema di Pitagora, che ora proveremo:

m) Siano P_1, P_2, P_3 punti distinti di π_q. Le rette P_1P_2 e P_2P_3 sono ortogonali se, e soltanto se, risulta:

$$N(P_1, P_2) + N(P_2, P_3) = N(P_1, P_3). \tag{4.11}$$

Dimostrazione. Sia $P_i = (x_i, y_i)$, $i = 1, 2, 3$. Un facile calcolo mostra che la retta P_1P_2 è ortogonale alla retta P_2P_3 se, e soltanto se, risulta:

$$(x_1 - x_2)(x_2 - x_3) = \theta(y_1 - y_2)(y_2 - y_3)\ . \tag{4.12}$$

D'altra parte la (4.11) equivale alla:

$$(x_1 - x_2)^2 - \theta(y_1 - y_2)^2 + (x_2 - x_3)^2 - \theta(y_2 - y_3) = (x_1 - x_3)^2 - \theta(y_1 - y_3)^2 \tag{4.13}$$

e cioè alla (4.12), a cui appunto si perviene esplicitando la (4.13). Onde l'asserto.

Nel piano euclideo π_q si può sviluppare tutta la geometria analitica in modo analogo al caso classico. Daremo alcuni esempi al riguardo.

Definiscesi norma di un punto P_o da una retta r, $N(P_o, r)$, la norma di P_o dal punto P_1 d'intersezione di r con la retta per P_o ortogonale ad r. Se r ha equazione $ax+by+c = 0$ e $P_o = (x_o, y_o)$, un facile calcolo mostra che è:

$$N(P_o, r) = \frac{\theta}{(\theta a^2 - b^2)} (ax_o + by_o + c)^2 \tag{4.14}$$

Definiscesi asse di $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ il luogo dei punti $P(x, y)$ di π_q che hanno uguale norma da P_1 e da P_2. Si constata facilmente che tale luogo è la retta di equazione:

$$x(x_1 - x_2) - y\theta(y_1 - y_2) - \frac{1}{2}\left[x_1^2 - x_2^2 - \theta(y_1^2 - y_2^2)\right] = 0\,, \tag{4.15}$$

cioè è la retta ortogonale alla P_1P_2 per il punto medio M tra P_1 e P_2. Ne segue anche che il punto medio M tra due punti P_1, P_2 coincide con l'unico punto della retta P_1P_2 che ha uguale norma da P_1 e da P_2.

Siano r ed r' due rette incidenti di equazioni $ax+by+c = 0$ ed $a'x+b'y+c'=0$. Il luogo dei punti $P(x, y)$ di π_q ad uguale norma da r e da r' ha equazione:

$$(ax + by + c)^2 = \left(\frac{\theta a^2 - b^2}{\theta a'^2 - b'^2}\right)(a'x + b'y + c')^2 \tag{4.16}$$

Due casi sono possibili a seconda che si abbia:

$$\frac{\theta a^2 - b^2}{\theta a'^2 - b'^2} \in \square' \qquad \text{oppure} \qquad \frac{\theta a^2 - b^2}{\theta a'^2 - b'^2} \in \not\square \tag{4.17}$$

Nel primo caso il luogo suddetto è costituito dalle due rette di equazioni:

$$ax + by + c = \pm\sqrt{\frac{\theta a^2 - b^2}{\theta a'^2 - b'^2}}\,(a'x + b'y + c')\,, \tag{4.18}$$

esse prendono il nome di bisettrici delle rette r ed r'. Nel secondo caso il luogo suddetto è costituito del solo punto d'incontro delle due rette, diremo allora che r ed r' non ammettono bisettrici. Se r ed r' sono ortogonali è soddisfatta la (4.9). Da essa si ha:

$$\frac{\theta a^2 - b^2}{\theta a'^2 - b'^2} = -\theta\left(\frac{a}{b'}\right)^2, \text{ se } b' \neq 0, \text{ oppure } \frac{\theta a^2 - b^2}{\theta(a')^2 - (b')^2} = -\frac{b^2}{\theta a'^2}, \text{ se } b'=0.$$

In ogni caso dunque l'elemento $(\theta a^2 - b^2)/(\theta a'^2 - b'^2)$ è un quadrato in G_q se, e soltanto se, $-\theta$ è un quadrato in G_q e cioè (essendo $\theta \in \not\square$) se, e soltanto se, -1 è un non quadrato in G_q. D'altra parte si prova facilmente che in G_q risulta:

$$-1 \in \not\square \iff q \equiv -1 \bmod 4. \tag{4.19}$$

Ne segue che:

n) Nel piano euclideo π_q due rette ortogonali ammettono bisettrici se, e soltanto se, $-1 \in \square$ in G_q, cioè se, e soltanto se, $q \equiv -1 \bmod 4$.

Osserviamo che, se $q \equiv -1 \bmod 4$, può scegliersi $\theta = -1$ (in virtù della eq. (4.19)). Le formule precedentemente stabilite si semplificano allora notevolmente riducendosi formalmente a quelle classiche.

I.5. - Circonferenze e movimenti in un piano euclideo su G_q, q dispari. -

Definiscesi circonferenza di un piano euclideo π_q, avente centro in un punto $C(\alpha,\beta)$ di π_q e norma $h(\in G_q)$, il luogo dei punti di π_q aventi norma h da C. Una circonferenza di centro $C(\alpha,\beta)$ e norma h ha dunque equazione:

$$(x-\alpha)^2 - \theta(y-\beta)^2 = h. \tag{5.1}$$

La (5.1) può anche scriversi nella forma:

$$x^2 - \theta y^2 - 2\alpha x + 2\beta\theta y + \gamma = 0 \tag{5.2}$$

ove si è posto:

$$\gamma = \alpha^2 - \theta\beta^2 - h. \tag{5.3}$$

Viceversa ogni equazione (5.2), al variare comunque di α, β, γ in G_q, è l'equazione di una circonferenza di centro (α,β) e norma $h = \alpha^2 - \theta\beta^2 - \gamma$. Ne segue che le circonferenze di π_q sono in numero di q^3.

Se $h = 0$, la circonferenza (5.1) si riduce al solo punto $C(\alpha,\beta)$. Nel seguito supporremo sempre $h \neq 0$. Comunque in ogni caso una circonferenza possiede sempre almeno un punto (cofr. prop. g), n. 2).

Il centro di una circonferenza $\mathscr{C}$ è centro di simmetria per essa. Come nel caso classico si prova che ogni retta di π_q o non ha punti in comune con $\mathscr{C}$ (retta esterna a $\mathscr{C}$) o ha due punti distinti in comune con $\mathscr{C}$ (retta secante $\mathscr{C}$) oppure incontra $\mathscr{C}$ in un unico punto T (retta tangente in T a $\mathscr{C}$); inoltre che se P_o è un punto di $\mathscr{C}$ (certamente esistente per la prop. g), n. 2), delle $q+1$ rette per P_o, esattamente una è tangente in P_o a $\mathscr{C}$ e coincide con la retta per P_o ortogonale alla CP_o, le altre sono tutte secanti $\mathscr{C}$ in P_o ed in un ulteriore punto $P(\neq P_o)$.

Ne segue che:

o) I punti di una circonferenza $\mathscr{C}$ (con norma $h \neq 0$ e centro $C(\alpha,\beta)$) sono in numero di $q+1$. La tangente in un punto $P_o(x_o, y_o)$ di $\mathscr{C}$ risulta la retta per P_o ortogonale alla retta CP_o ed ha quindi equazione:

$$(x-\alpha)(x_o-\alpha) - \theta(y-\beta)(y_o-\beta) = h. \tag{5.4}$$

Chiamasi movimento di un piano euclideo π_q una affinità di π_q che conserva la norma (cioè tale che, per ogni P_1, P_2 di π_q, risulta $N(P_1, P_2) = N(P_1', P_2')$, ove P_1',

P_2' sono i corrispondenti di P_1, P_2 nell'affinità). Evidentemente un movimento muta circonferenza in circonferenze e, in forza delle prop. m), del n. 4, conserva l'ortogonalità tra rette. Poichè l'identità, l'inverso di un movimento ed il prodotto di due movimenti sono movimenti, si ha che l'insieme dei movimenti di π_q è un gruppo (rispetto al prodotto operatorio), sottogruppo di quello affine, che denoteremo con M_q. Chiamasi geometria euclidea lo studio delle proprietà delle figure di π_q invarianti rispetto al gruppo M_q. Nella geometria euclidea di π_q dunque due figure si considerano uguali se esiste un movimento che muta l'una nell'altra.

Proponiamoci di determinare le equazioni di un movimento di π_q. Si tratta di imporre alle equazioni (3. 2) di una affinità di trasformare $x'^2 - \theta y'^2$ in $x^2 - \theta y^2$. A calcoli eseguiti si ottiene:

$$(5.6) \qquad a_{11}^2 - \theta a_{21}^2 = 1, \quad a_{12}^2 - \theta a_{22}^2 = -\theta, \quad a_{11}a_{12} - \theta a_{21}a_{22} = 0$$

Risolvendo il sistema (5. 6), ove si ponga:

$$(5.7) \qquad a_{11} = \lambda, \qquad a_{21} = \mu,$$

si ottiene:

$$(5.8) \qquad a_{11} = \lambda, \quad a_{12} = \pm\theta\mu, \quad a_{21} = \mu, \quad a_{22} = \pm\lambda, \quad \lambda^2 - \theta\mu^2 = 1,$$

ove vanno presi o i segni inferiori o i superiori simultaneamente. Ne segue che:

p) Le equazioni di un qualsiasi movimento di π_q sono date da:

$$(5.9) \qquad x' = \lambda x \pm \theta\mu y + a_1, \qquad y' = \mu x \pm \lambda y + a_2$$

ove vanno presi simultaneamente o i segni superiori o quelli inferiori e λ, μ sono due qualunque elementi di G_q soddisfacenti alla:

$$(5.10) \qquad \lambda^2 - \theta\mu^2 = 1.$$

Il determinante, Δ, dei coefficienti di un movimento (5. 9) risulta dato, in forza delle (5. 10), da: $\Delta = \pm 1$, a seconda che nella (5. 9) si prendono i segni superiori o inferiori. I movimenti si dividono perciò in diretti od inversi a seconda che $\Delta = 1$ o $\Delta = -1$. I movimenti diretti costituiscono un sottogruppo M_q^+ di M_q di indice due in M_q.

Si osservi che l'equazione (5. 10), nel piano π_q di coordinate (λ, μ), rappresenta la circonferenza di centro l'origine e norma 1. Essa possiede dunque $q+1$ punti, per la prop. o). Ne segue che i movimenti diretti sono esattamente in numero di $(q+1)q^2$ (infatti un siffatto movimento si ottiene fissando una coppia (λ, μ) di G_q soddisfacente alla (5. 10), e di tali coppie ve ne sono $q+1$, ed una qualsiasi coppia (a_1, a_2) di G_q, e di tali coppie ve ne sono q^2) e così per quelli inversi. Si è così provato che:

q) I movimenti di π_q sono in numero di $2(q+1)q^2$; precisamente $(q+1)q^2$ diretti ed altretanti inversi, cioè:

$$(5.11) \qquad |M_q| = 2(q+1)q^2, \qquad |M_q^+| = (q+1)q^2.$$

Si prova facilmente che:

r) Dati comunque due coppie di punti (P_1, P_2) e (P_1', P_2'), tali che $N(P_1, P_2) = N(P_1', P_2') \neq 0$, esistono esattamente due movimenti che mutano P_1 in P_1' e P_2 in P_2', l'uno diretto, l'altro inverso.

I. 6. - Proprietà affini e metriche delle coniche su G_q (q dispari). -

Analogamente al caso classico si passa dal piano π_q al piano ampliato π_q^*, aggiungendo a π_q i suoi punti impropri o direzioni di π_q, e si introducono coordinate omogenee (x_1, x_2, x_3) in π_q^* ($x_3 = 0$ essendo l'equazione della retta impropria).

Definiscesi conica di π_q^* il luogo dei punti di π_q^* le cui coordinate omogenee soddisfano alla equazione a coefficienti in G_q (q dispari):

$$(6.1) \qquad \sum_{i,j}^{1,2,3} a_{ij} x_i x_j = 0 , \qquad a_{ij} = a_{ji}$$

Per la proposizione h) del n. 2 si ha che ogni conica possiede almeno un punto. Nel seguito ci occuperemo esclusivamente di coniche non degeneri (cioè tali che $\det \| a_{ij} \| \neq 0$). Per una tale conica $\mathcal{C}$ una qualsiasi retta del piano o è secante (cioè incontra $\mathcal{C}$ in due punti distinti) o è esterna (se non ha punti in comune con $\mathcal{C}$) oppure è tangente a $\mathcal{C}$ in un punto T (se incontra $\mathcal{C}$ solamente in T). Inoltre, come nel caso classico, si prova che se P_0 è un punto di $\mathcal{C}$ (certamente esistente per la prop. h) del n. 2) delle $q+1$ rette per P_0 una è tangente in P_0 a $\mathcal{C}$, le altre q sono secanti $\mathcal{C}$, in P_0 ed in un punto $P \neq P_0$. Ne segue che:

s) I punti di una qualsiasi conica non degenere di π_q^* sono in numero di $q+1$ ed a tre a tre non allineati.

La proporzione precedente si può invertire sussistendo il seguente teorema di B. Segre:

t) Ogni insieme di $q+1$ punti di π_q^* (q dispari) di cui mai tre allineati risulta una conica non degenere.

In modo analogo al caso classico si definisce la polarità rispetto ad una conica $\mathcal{C}$, la polare di un punto $P(y_1, y_2, y_3)$ rispetto a $\mathcal{C}$ essendo la retta di equazione:

$$(6.2) \qquad \sum_{i \neq j}^{1,2,3} a_{ij} y_i x_j = 0 .$$

Se $P \in \mathcal{C}$ la (6.2) risulta la tangente in P alla $\mathcal{C}$.

Una conica $\mathcal{C}$ dicesi ellisse, parabola, iperbole a seconda che la retta impropria, $x_3 = 0$, sia esterna, tangente, secante la conica $\mathcal{C}$. Nei tre casi si ha:

$$(6.3)\qquad \begin{cases} a_{12}^2 - a_{11}a_{22} \in \emptyset & \text{, ellisse} \\ a_{12}^2 - a_{11}a_{22} = 0 & \text{, parabola} \\ a_{12}^2 - a_{11}a_{22} \in \square & \text{, iperbole.} \end{cases}$$

Le nozioni e le proprietà affini delle coniche (centro, diametri, diametri coniugati, asintoti) si introducono e si stabiliscono in modo del tutto analogo al caso classico e non sussistono risultati sostanzialmente nuovi rispetto a quel caso.

Passiamo alle proprietà metriche delle coniche. L'asse di una conica si definisce come diametro coniugato alla propria direzione ortogonale, cioè come asse di simmetria ortogonale di $\mathcal{C}$. Le intersezioni di $\mathcal{C}$ con gli assi diconsi vertici.

Una parabola possiede sempre uno ed uno solo asse, dato dalla polare del punto improprio in direzione ortogonale ai diametri (che sono tutti tra loro paralleli). Si può sempre effettuare un movimento in modo da far coincidere l'asse della parabola e la sua tangente nel vertice rispettivamente con l'asse x e l'asse y, l'equazione della parabola si riduce allora alla ben nota forma canonica:

$$(6.4)\qquad y^2 = 2ax .$$

Si verifica facilmente che essa è il luogo dei punti di π_q ad uguale norma dal punto $F(-a\theta/2, 0)$ e dalla retta $d: x = a\theta/2$. Il punto F e la retta d prendono il nome di fuoco e direttrice della parabola.

Occupiamoci ora del problema dell'esistenza degli assi per una conica $\mathcal{C}$ a centro. Non è restrittivo supporre che il centro di $\mathcal{C}$ sia l'origine O(0, 0) (in quanto mediante un movimento ci si può sempre ridurre a questo caso). L'equazione di $\mathcal{C}$ risulta allora:

$$(6.5)\qquad a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + a_{33} = 0$$

Sia $y = mx$ un diametro di $\mathcal{C}$, la polare del suo punto improprio (1, m, 0) ha equazione:

$$(6.6)\qquad (a_{11} + a_{12}m)x + (a_{12} + a_{22}m)y = 0$$

Essa è ortogonale alla $y = mx$ se, e soltanto se, risulta:

$$\theta\, m(a_{11} + a_{12}m) + (a_{12} + a_{22}m) = 0$$

cioè se, e soltanto se, è:

$$(6.7)\qquad \theta a_{12}m^2 + m(a_{22} + \theta a_{11}) + a_{12} = 0 .$$

Gli assi di $\mathcal{C}$ hanno dunque coefficienti angolari m soddisfacenti alla (6.7). Se la (6.7) è identicamente soddisfatta, cioè $a_{12} = 0$, $a_{22} = -\theta a_{11}$, nel qual caso $\mathcal{C}$ è una circonferenza, ogni diametro di $\mathcal{C}$ è un asse. In caso contrario, se è $a_{12} = 0$ (e

quindi $a_{22} + \theta a_{11} \neq 0$) $\mathcal{C}$ ha esattamente due assi dati dall'asse x e l'asse y, se è $a_{12} \neq 0$ la conica $\mathcal{C}$ ha esattamente due assi (tra loro ortogonali) oppure non possiede assi a seconda che si abbia:

(6.8) $$(a_{22} + \theta a_{11})^2 - 4\theta a_{12}^2 \in \square'$$

oppure

(6.9) $$(a_{22} + \theta a_{11})^2 - 4\theta a_{12}^2 \in \not\square$$

Si noti che, qualsiasi sia q, esistono sempre degli elementi a_{11}, a_{12}, a_{22} di G_q soddisfacente alla (6.9) (cfr. n. 2), ne segue che esistono sempre, qualsiasi sia q, coniche prive di assi di simmetria. Si ha dunque che:

Una qualsiasi conica a centro o è una circonferenza, ed allora ogni suo diametro è un asse, oppure ammette esattamente due assi ortogonali o non possiede assi di simmetria.

Nel caso delle coniche a centro dotate di assi, si può sempre effettuare un movimento che faccia coincidere tali assi con l'asse x e l'asse y. Si ottengono allora le seguenti forme canoniche, a seconda che sia $-1 \in \not\square$, cioè $q \equiv -1 \bmod 4$, oppure $-1 \in \square$, cioè $q \not\equiv -1 \bmod 4$:

$-1 \in \not\square$

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \qquad \text{ellisse (con 4 vertici),}$$

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \qquad \text{iperbole (con due vertici).}$$

$-1 \in \square$

$$\frac{x^2}{a^2} - \theta\frac{y^2}{b^2} = 1 \qquad \text{ellisse (con due vertici),}$$

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \qquad \text{iperbole (con 4 vertici),}$$

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 0 \qquad \text{iperbole (senza vertici).}$$

Si può facilmente provare che le coniche datate di assi si possono definire come luogo dei punti P di π_q per cui risulti costante (eccentricità) il rapporto tra le norme di P da un punto F (fuoco) e da una retta d (direttrice).

In modo analogo al caso classico si definisce equilatera una iperbole con gli asintoti ortogonali. Si prova facilmente che la condizione perchè una iperbole sia equilatera è data da:

(6.10) $$\theta a_{11} - a_{22} = 0.$$

Poichè gli assi sono le bisettrici degli asintoti di una iperbole si ha che: una iperbole equilatera possiede assi di simmetria se, e soltanto se, risulta $-1 \in \not\square$ cioè

$q \equiv -1 \bmod 4$ (cfr. n. 4).

Quanto esposto nei n. 4, 5, 6 si può estendere facilmente al caso di un qualsiasi campo K (anche infinito) di caratteristica $\neq 2$, purchè possega un elemento θ non quadrato in K.

RIFERIMENTI. -

(1) - P. Dembowski, Finite geometries, Ergebnisse der Math. (Springer, 1968).

(2) - B. Segre, Lectures on modern geometry (Cremonese, 1961).

(3) - G. Tallini, Le geometrie di Galois e le loro applicazioni alla statistica e alla teoria dell'informazione, Rend. Mat. 19, 379 (1960).

II. - APPLICAZIONI ALLA FISICA. -

(A cura di E. G. Beltrametti, Istituto di Fisica dell'Università di Genova).

II. 1. - In queste lezioni mi propongo di esaminare, in modo necessariamente sommario, talune applicazioni alla fisica delle nozioni di campo e geometria di Galois, nozioni esaurientemente presentate nelle precedenti lezioni del Prof. G. Tallini. La bibliografia che verrà tenuta presente, ma non egualmente utilizzata, inizia con alcuni lavori di Jarnefelt e Kustaanheimo[1] a cui seguono articoli di Coish[2], Shapiro[3], Kadyshevskii[4], Joos[5], Ahmaraara[6] e, più recentemente, contributi dello scrivente in collaborazione con Blasi[7, 8]. Elemento comune a questa bibliografia è la domanda: è possibile una descrizione dello spazio fisico mediante una geometria finita (o di Galois)? Una considerazione che sembra aver spesso stimolato questa domanda consiste nel fatto che una teoria dinamica costruita su una geometria finita è strutturalmente immune dalla solita difficoltà delle divergenze, poichè ogni integrale lascia il posto a somme finite. La domanda avanzata sopra propone subito il problema di individuare una qualche regola di corrispondenza fra una descrizione basata su una geometria finita e gli schemi classici: questo problema appare non banale se si tiene presente che un campo finito $GF(p^n)$ non è ordinabile, cosicchè una geometria di Galois, i cui punti hanno coordinate in $GF(p^n)$, non possiede le usuali proprietà metriche.

Jarnefelt e Kustaanheimo[1] hanno proposto una via d'uscità per tale difficoltà assumendo che la fisica richieda una nozione di spazio-tempo solo localmente in corrispondenza con la usuale nozione basata sul continuo, e mostrando che un campo di Galois d'ordine opportuno è localmente ordinabile. Con ciò si intende che, se l'ordine del campo (che d'ora in poi, e principalmente per ragioni di semplicità di notazioni, supporremo primo) soddisfa una condizione del tipo:

$$p \equiv 3 \pmod 4, \tag{1}$$

allora esiste nel campo una catena "Euclidea" di N elementi consecutivi transitivamente ordinabili rispetto a

$$x > y \quad \text{se} \quad (x-y) \in \square' \; ; \quad x < y \quad \text{se} \quad (x-y) \in \not\square$$

(si sono usate le notazioni del paragrafo 2 delle precedenti lezioni). Una stima di N conduce approssimativamente a $N \sim \ln p$. I punti dello spazio (o dello spazio-tempo) che hanno coordinate nella catena Euclidea costituiscono dunque una sorta di reticolo che, al crescere di p e quindi di N, contiene un cosi grande numero di punti da divenire empiricamente equivalente ad un continuo, se si ammette di non saper misurare distanze arbitrariamente piccole (diciamo, ad esempio, minori di $\sim 10^{-15}$ cm). Naturalmente la catena Euclidea non ha le proprietà algebriche di un campo e ciò può portare a qualche difficoltà nel precisare regole di corrispondenza con la descrizione usuale.

Occorre d'altra parte osservare che se per distanze molto minori di quelle nucleari si rinunzia ai concetti classici, la nozione di spazio-tempo esiste nella misura in cui esista una teoria coerente ed in accordo con l'esperienza. Una formu

lazione sicura delle regole di corrispondenza con la descrizione usuale dovrebbe dunque seguire e non precedere una tale teoria (questo è l'atteggiamento sottolineato nel rif. (3)).

Nel seguito assumeremo senz'altro la condizione (1): essa consente un minimo di analogia fra le operazioni algebriche in GF(p) è quelle nel campo dei reali. Invero da essa discende facilmente[3, 7]:

$$x \in \square' \iff -x \in \not\square ,$$

ossia l'opposto di un elemento positivo (quadrato) è nagativo (non-quadrato) e viceversa.

Infine è opportuno notare che la (1) consente in particolare di riguardare $GF(p^2)$ come la naturale "complessificazione" di GF(p), come discusso nel primo paragrafo delle precedenti lezioni; si osservi che, posto $z = x + iy$, con $z \in GF(p^2)$, $x, y \in GF(p)$, $i^2 = -1$, si ha:

$$z^* = x - iy = z^p . \tag{2}$$

II. 2. - Ad eventuali tentativi intesi a costruire una teoria dinamica basata su una geometria finita, sembra ragionevole premettere uno studio orientativo sulle novità che tale geometria comporta al livello delle proprietà di simmetria connesse con trasformazioni spazio-temporali.

In quest'ordine di idee definiamo il gruppo proprio di Lorentz L(4, p) come il gruppo delle sostituzioni lineari invertibili

$$x'_\mu = \sum_{\nu=0}^{3} 1_{\mu\nu} x_\nu \quad ; \quad \mu = 0, 1, 2, 3 ; \; x_\mu, 1_{\mu\nu} \in GF(p) ; \det 1 = +1 , \tag{3}$$

che lasciano invariata la forma quadratica $x_0^2 - x_1^2 - x_2^2 - x_3^2$ (1 indica la matrice 4×4 con elementi $1_{\mu\nu}$). Il sottogruppo R(3, p) delle rotazioni proprie in 3 dimensioni è similmente formato dalle sostituzioni:

$$x'_i = \sum_{j=1}^{3} r_{ij} x_j ; \quad i = 1, 2, 3 ; \; x_i, \; r_{ij} \in GF(p) ; \quad \det r = +1 , \tag{4}$$

che lasciano invariato $x_1^2 + x_2^2 + x_3^2$.

L(4, p) e R(3, p) sono gruppi finiti (si noti che la loro definizione non coincide con quella dei rif. (2) e (3) dove si ammette anche un possibile cambiamento di segno della forma quadratica); i loro ordini possono essere ottenuti con metodi standard[9] e risultano:

$$\Omega_{L(4,p)} = p^2(p^4 - 1) , \qquad \Omega_{R(3,p)} = p(p^2 - 1).$$

Si deve osservare che in questa versione finita del gruppo di Lorentz non è possibile separare il sottogruppo ortocrono: ciò è strettamente connesso col fatto che, in GF(p), la somma di elementi positivi (quadrati) non è necessariamente

positiva (cosicchè dalla relazione $l_{oo}^2 = 1 + l_{o1}^2 + l_{o2}^2 + l_{o3}^2$ non discende necessariamente l'alternativa usuale $l_{oo} > 1$ o $l_{oo} < -1$). $L(4, p)$ contiene dunque anche l'analogo delle transformazioni non ortocrone ed in particolare il prodotto dell'inversione spaziale per quella temporale : su questo aspetto insolito torneremo nel seguito.

Dal punto di vista fisico l'interesse è principalmente legato alle rappresentazioni di questi gruppi : a questo scopo risulterà utile, come nel caso classico, stabilire omomorfismi con gruppi di matrici 2 x 2. Si consideri per questo il gruppo $SL^{\pm}(2, p^2)$ di matrici 2 x 2 a elementi in $GF(p^2)$:

$$(4) \qquad a = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL^{\pm}(2, p^2); \quad \alpha, \beta, \gamma, \delta \in GF(p^2), \quad \det a = \pm 1 .$$

Si tratta di un gruppo finito il cui ordine risulta $2\Omega_{L(4,p)}$. Interesserà anche considerare il sottogruppo $SU^{\pm}(2, p^2)$ formato dalle matrici :

$$u = \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \in SU^{\pm}(2, p^2); \quad \alpha, \beta \in GF(p^2), \quad \det u = \pm 1 ,$$

e che ha ordine $2\Omega_{R(3,p)}$.

Si può dimostrare[7] che esiste un omomorfismo 1 a 2 fra $L(4, p)$ e $SL^{\pm}(2, p^2)$; come caso particolare $R(3, p)$ risulta omomorfo a $SU^{\pm}(2, p^2)$. Esplicitamente, l'omomorfismo è fornito dalla relazione :

$$(5) \qquad \hat{x}' = (\det a)\, a\, \hat{x}\, a^{\dagger}, \qquad \text{con} \qquad \hat{x} = \begin{pmatrix} x_o + x_3 & x_1 - ix_2 \\ x_1 + ix_2 & x_o - x_3 \end{pmatrix}$$

($a^{\dagger}$ è la matrice coniugata hermitiana di a) e mostra che le due matrici a, - a hanno la stessa imagine in $L(4, p)$.

E' opportuno sottolineare la differenza con il caso classico nel quale si ha un omomorfismo 1 a 2 fra il gruppo di Lorentz e le matrici complesse 2 x 2 con determinante +1. Osserviamo anche che, l'assenza di un sottogruppo ortocrono implica che il prodotto dell'inversione spaziale per quella temporale ha immagine in $SL^{\pm}(2, p^2)$: tale immagine è offerta dalle due matrici $\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ che, come era da attendersi, hanno determinante - 1.

II. 3. - Dobbiamo ora fare una scelta per il campo numerico su cui realizzare le rappresentazioni del gruppo di Lorentz e delle rotazioni ; in altre parole dobbiamo decidere su quale campo numerico vogliamo definire lo spazio degli stati fisici (funzioni d'onda). Nello schema della meccanica quantistica questa scelta appare, a priori, indipendente dalla scelta del campo su cui si sono definite le coordinate spaziali e temporali. La prima tentazione potrebbe dunque essere quella di adottare, come di solito, il campo dei numeri complessi ; avremmo cosi a che fare con rappresentazioni ordinarie di gruppi finiti e potremmo utilizzare il bagaglio convenzionale sulla teoria delle rappresentazioni. Tale scelta appare però priva di interesse fisico : infatti è stato dimostrato da Steinberg[10] che la dimensione minima

delle rappresentazioni (non banali) su $\mathcal{C}$ del gruppo $SL^{+}(2, p^2)$ è $p^2 - 1$, ossia un valore inaccettabilmente grande, dal momento che in fisica desideriamo disporre anche di spinori a due componenti, di quadrivettori, etc. Tenuto conto di questa difficoltà(x), appare naturale considerare rappresentazioni su $GF(p^2)$, il campo che, nei riguardi di $GF(p)$, ha il ruolo dei complessi nei riguardi dei reali. Poichè $GF(p^2)$ ha caratteristica $p \neq 0$, le rappresentazioni in questione rientrano in quelle che la letteratura matematica chiama "rappresentazioni modulari"(11). Nel lavorare con rappresentazioni di questo tipo si deve rinunziare ad alcuni strumenti abituali: ad esempio il "lemma di Schur" diventa condizione necessaria ma non più sufficiente per l'irriducibilità; le rappresentazioni riducibili non sono necessariamente decomponibili; le rappresentazioni (di gruppi finiti) non sono più, in generale, equivalenti a rappresentazioni unitarie; l'uguaglianza fra il numero di classi di equivalenza del gruppo e il numero di rappresentazioni irriducibili richiede nuove precisazioni(11, 8).

La forma esplicita delle rappresentazioni di $SL^{\pm}(2, p^2)$ su $GF(p^2)$ può essere facilmente dedotta con il solito metodo di Weyl e si può dimostrare(8) che tutte e sole rappresentazioni irriducibili sono date da:

$$D^{(j,k;\varepsilon)}(a) = (\det a)^{\varepsilon}\ D^{(j)}(a) \otimes \left[D^{(k)}(a)\right]^{*}, \quad \begin{cases} \varepsilon = 0, 1 \\ j, k = 0, 1/2, 1, \ldots, \frac{p-1}{2} \end{cases} \tag{6}$$

dove $D^{(j)}(a)$ è una matrice di dimensione $2j+1$ con elementi:

$$D^{(j)}_{m,m'}(a) = \frac{N^{(j)}_{m}}{N^{(j)}_{m'}} \sum_{\lambda=\max(0,\, m-m')}^{\min(j+m,\, j-m')} \binom{j+m}{\lambda} \binom{j-m}{\lambda+m'-m} \cdot \tag{6'}$$

$$\cdot\ \alpha^{j-m'-\lambda}\, \delta^{j+m-\lambda}\, \beta^{\lambda}\, \gamma^{\lambda-m+m'}$$

($N^{(j)}_{m}$ sono fattori di normalizzazione per il momento arbitrari, definiti in $GF(p^2)$).

Restrigendosi al sottogruppo $SU^{+}(2, p^2)$ si verifica facilmente che $(D^{(k)}(u))^{*}$ è equivalente a $D^{(k)}(u)$, cosicchè le rappresentazioni irriducibili ed inequivalenti di $SU^{\pm}(2, p^2)$ corrispondono a porre $k = 0$ (oltre che $\delta = \alpha^{*}$, $\gamma = -\beta^{*}$) nella (6) e (6').

Si noti che gli indici di spin j, k sono limitati superiormente da $(p-1)/2$: se si supera questo limite si ottengono rappresentazioni riducibili.

Rispetto al caso ordinario basato sul continuo, la novità più evidente di queste rappresentazioni modulari è la comparsa del parametro ε a due valori necessario per distinguere fra le due possibili rappresentazioni inequivalenti di uguale dimensionalità.

Tale parametro è dunque ineliminabile nella classificazione delle rappresentazioni vettoriali di $L(4, p)$ e $R(3, p)$ che possono dedursi, al solito modo, dalle (6), (6') utilizzando l'omomorfismo (5). Tuttavia, per quanto riguarda l'interpretazione fisica, potremmo dire che esso è irrilevante, poichè gli stati fisici sono de

---

(x) - Questa difficoltà non è stata tenuta in debito conto nel rif. (6).

terminati a meno di un fattore di fase, o, in altre parole, la fisica richiede rappresentazioni "di raggio" (anche chiamate "proiettive") piùttosto che rappresentazioni vettoriali (è noto che in taluni casi, ad esempio per il gruppo classico di Galilei, solo le rappresentazioni di raggio hanno significato fisico). Torneremo su questo punto più avanti. Nel prossimo paragrafo vedremo comunque che la comparsa di un tale numero quantico a due valori riapparirà in modo essenziale nello studio del gruppo di Lorentz improprio.

Nel seguito ci limiteremo ad analizzare le proprietà delle rappresentazioni corrispondenti a "spin 1/2"; a questo proposito servirà tenere presente che, con una scelta opportuna dei coefficienti di normalizzazione nella (6')

$$D^{(1/2,\,0;\,\varepsilon)}(a) = (\det a)^{\varepsilon}\, a\,. \tag{7}$$

II. 4. - Passiamo ora a considerare il gruppo di Lorentz improprio $\mathcal{L}(4,p)$, ottenuto da quello proprio $L(4,p)$ aggiungendo l'operazione P di inversione spaziale. Ci occuperemo delle rappresentazioni di spin 1/2 di tale gruppo. E' noto dalla trattazione convenzionale che non esiste una rappresentazione bidimensionale di P: ciò può riconoscersi dal fatto che P induce, sulla base 2 x 2 di coordinate data da x (vedi (5)), una trasformazione tipicamente non lineare:

$$\hat{x} \xrightarrow{P} \eta\, x^{*} \eta^{-1}\,, \qquad \eta = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Per ottenere una rappresentazione di $P^{(o)}$ occorre adottare una base 4 x 4, ad esempio:

$$\hat{y} = \begin{pmatrix} \hat{x} & 0 \\ 0 & \eta\, \hat{x}^{*}\, \eta^{-1} \end{pmatrix} \tag{8}$$

su cui P induce la transformazione lineare:

$$\hat{y} \xrightarrow{P} \gamma_o\, \hat{y}\, \gamma_o^{\dagger}\,, \qquad \text{con } \gamma_o = \begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix}. \tag{9}$$

Vogliamo ora precisare la trasformazione indotta dal gruppo proprio $L(4,p)$ sulla nuova base $\hat{y}$. Tenendo conto della (5) e della (7) si verifica facilmente che:

$$\hat{y} \xrightarrow{L(4,p)} (\det a)\, S(a)\, \hat{y} \left[S(a)\right]^{\dagger} \tag{10}$$

dove si è posto:

$$S(a) = (\det a)^{\varepsilon} \begin{pmatrix} a & 0 \\ 0 & \theta_a (\det a)\, a^{\dagger\,-1} \end{pmatrix}$$

(o) - Si noti che a tale rappresentazione si rinunzia nel rif. (3).

e, per la proprietà di gruppo, il fattore numerico θ_a deve soddisfare

$$\theta_a \theta_{a'} = \theta_{aa'} .$$

Il fattore θ_a deve dunque fornire una rappresentazione unidimensionale del gruppo $SL^{\pm}(2, p^2)$; abbiamo di consequenza dalla (6):

$$\theta_a = (\det a)^e , \qquad e = 0, 1$$

(si noti che la possibilità di avere $\theta_a \neq 1$ non ha analogo nel caso usuale del continuo poichè in tal caso intervengono soltanto matrici a determinante +1).

Riassumendo, possiamo precisare la (10) mediante:

$$(10') \qquad S(a) = S^{(\varepsilon, e)}(a) = (\det a)^{\varepsilon} \begin{pmatrix} a & 0 \\ 0 & (\det a)^{e+1} a^{\dagger -1} \end{pmatrix} .$$

La generica rappresentazione di spin 1/2 del gruppo improprio $\mathcal{L}(4, p)$ è dunque fornita da $S^{(\varepsilon, e)}(a)$ per il gruppo proprio e da γ_o per l'inversione P. Al variare di ε ed e abbiamo dunque quattro rappresentazioni (vettoriali) inequivalenti. Dobbiamo a questo punto domandarci se è possibile attribuire un significato fisico a questi nuovi numeri quantici. Per quanto riguarda ε si può ripetere l'osservazione fatta alla fine del paragrafo II. 3: se gli spinori su cui operano queste rappresentazioni sono definiti a meno di un fattore di fase, ossia se siamo interessati a rappresentazioni di raggio e non a quelle vettoriali, allora ε è irrilevante. Invero, $S^{(o, e)}(a)$ e $S^{(1, e)}(a)$ sono equivalenti dal punto di vista delle rappresentazioni di raggio[12]. Nel seguito adotteremo senz'altro rappresentazioni di raggio, anche perchè sembra più significativo esaminare fino a che punto i nuovi numeri quantici che intervengono nella versione finita del gruppo di Lorentz siano inelimi nabili.

Porremo allora

$$(11) \qquad S^{(e)}(a) = \chi_a \begin{pmatrix} a & 0 \\ 0 & (\det a)^{e+1} a^{\dagger -1} \end{pmatrix}$$

e sceglieremo χ_a in modo da recuperare, in analogia col caso classico, l'unitarietà formale della rappresentazione quando ristretta a $SU^{\pm}(2, p^2)$, ossia alle rotazioni. Poichè $un^{+} = (\det u)\mathbb{1}$, sceglieremo per χ_a una soluzione dell'equazione

$$(11') \qquad \chi_a \chi_{\bar{a}}^{*} = \det a .$$

Cosi facendo abbiamo la regola di moltiplicazione:

$$S^{(e)}(a) \quad S^{(e)}(a') = \omega_{a, a'} \; S^{(e)}(aa'), \qquad \omega_{a, a'} = \frac{\chi_a \chi_{a'}}{\chi_{aa'}}$$

tipica delle rappresentazioni di raggio, dal momento che i coefficienti $\omega_{a, a'}$ soddisfano le condizioni dovute[12]

$$\omega_{a, a'} \cdot \omega^{*}_{a, a'=1} , \qquad \omega_{aa', a''} \omega_{a, a'} = \omega_{a, a'a''} \omega_{a', a''}$$

scelte diverse della soluzione dell'equazione (11') corrispondono a rappresentazioni di raggio equivalenti[7, 8].

Se d'un lato è stato possibile sbarazzarci del numero quantico ϵ, altrettanto non possiamo fare con il numero e, la cui presenza appare ineliminabile, anche al livello delle rappresentazioni di raggio (vedi (11)). Abbiamo dunque a che fare due diversi campi spinoriali (di Dirac) $\psi^{(o)}$, $\psi^{(1)}$ che si trasformano rispettivamente secondo la rappresentazione

$$\left\{S^{(o)}(a),\ \gamma_o\right\} \qquad \text{oppure} \qquad \left\{S^{(1)}(a),\ \gamma_o\right\}.$$

Nel prossimo paragrafo esamineremo le differenti proprietà di questi due campi nei riguardi delle consuete correnti covarianti.

II. 5. - Consideriamo le correnti sesquilineari nei due spinori di Dirac

$$\psi^{(e)\dagger} B_{(\tau)} \psi^{(e')} , \qquad e, e' = 0, 1 \tag{12}$$

dove $B_{(\tau)}$ è una matrice 4x4 la cui natura tensoriale è precisata dall'insieme di indici riassunto da (τ). Vogliamo esaminare se esistono matrici $B_{(\tau)}$ che rendono la corrente (12) covariante rispetto a $\mathcal{L}(4, p)$. Tenuto conto che, per definizione, $\psi^{(e)}$ si trasforma in $S^{(e)}(a)\psi^{(e)}$ sotto l'azione delle transformazioni di Lorentz proprie L(4, p), mentre si trasforma in $\gamma_o\psi^{(e)}$ sotto l'azione dell'inversione spaziale P, si conclude che la legge di trasformazione della (12) è:

$$\begin{aligned} &\psi^{(e)\dagger} B_{(\tau)} \varphi^{(e')} \xrightarrow{\ P\ } \psi^{(e)\dagger} \gamma_o B_{(\tau)} \gamma_o \varphi^{(e')} \\ &\psi^{(e)\dagger} B_{(\tau)} \varphi^{(e')} \xrightarrow{\ L(4,p)\ } \psi^{(e)\dagger} S^{(e)}(a) B_{(\tau)} S^{(e')}(a) \varphi^{(e')} \end{aligned} \tag{13}$$

Vediamo nell'ordine le varie possibilità:

a) Scalare - In tal caso $B_{(\tau)}$ è una matrice scalare B e la (12) deve essere invariante sia rispetto a L(4, p) che a P: quindi

$$\gamma_o B \gamma_o = B, \qquad S^{(e)\dagger}(a) B S^{(e')}(a) = B .$$

Si verifica facilmente[o] che queste equazioni sono soddisfatte (identicamente rispetto ad a) se, e solo se:

$$e = e' = 0 , \qquad B = \gamma_o , \tag{14.1}$$

a meno, ovviamente, di un fattore numerico di proporzionalità nell'espressione di B.

(o) - E' comodo, per il calcolo, pensare B scomposta in blocchi 2x2.

b) Pseudo-scalare - In tal caso occorre soddisfare le equazioni:

$$\gamma_o B \gamma_o = -B, \qquad S^{(e)\dagger}(a) B S^{(e')}(a) = B,$$

che implicano

(14.2) $$e = e' = 0, \qquad B = \gamma_o \gamma_5 ,$$

dove si è posto:

(15) $$\gamma_5 = i \begin{pmatrix} -\mathbb{1} & 0 \\ 0 & \mathbb{1} \end{pmatrix} .$$

c) Vettore - In questo caso $B_{(\tau)}$ verrà riscritta come B_μ, $\mu = 0, 1, 2, 3$. Le equazioni da soddisfare sono:

$$\gamma_o B_\mu \gamma_o = -(-1)^{\delta_{o\mu}} B_\mu, \quad S^{(e)\dagger} B_\mu S^{(e')}(a) = \frac{1}{2}(\det a) \sum_{\nu=0}^{3} \mathrm{Tr}(\sigma_\mu a \sigma_\nu a^\dagger) B_\nu ,$$

come può vedersi dalla (5) esplicitando la regola di trasformazione delle coordinate x_μ per trasformazioni di Lorentz proprie. Tali equazioni conducono a:

(14.3) $$e = e' = 0, 1 , \qquad B_\mu = \gamma_o \gamma_\mu ,$$

avendo posto:

(16) $$\gamma_1 = \begin{pmatrix} 0 & -\sigma_1 \\ \sigma_1 & 0 \end{pmatrix} \qquad \text{per } 1 = 1, 2, 3 .$$

d) Vettore assiale - Le equazioni sono:

$$\gamma_o B_\mu \gamma_o = (-1)^{\delta_{o\mu}} B_\mu , \qquad S^{(e)\dagger}(a) B_\mu S^{(e')}(a) = \frac{1}{2}(\det a) \sum_{\nu=0}^{3} \mathrm{Tr}(\sigma_\mu a \sigma_\nu a^\dagger) B_\nu$$

e sono soddisfatte se:

(14.4) $$e = e' = 0, 1 , \qquad B_\mu = \gamma_o \gamma_5 \gamma_\mu .$$

e) Tensore - (τ) indica ora due indici $\mu, \nu = 0, 1, 2, 3$ e le equazioni da soddisfare sono:

$$\gamma_o B_{\mu,\nu} \gamma_o = (-1)^{\delta_{o\mu} + \delta_{o\nu}} B_{\mu\nu} ,$$

$$S^{(e)\dagger}(a) B_{\mu,\nu} S^{(e')}(a) = \frac{1}{4} \sum_{\rho,\lambda=0}^{3} \mathrm{Tr}(\sigma_\mu a \sigma_\rho a^\dagger) \mathrm{Tr}(\sigma_\nu a \sigma_\lambda a^\dagger) B_{\rho,\lambda} ,$$

e risultano soddisfatte se, e solo se:

(14.5) $$e = e' = 0 , \qquad B_{\mu,\nu} = \gamma_o \gamma_\mu \gamma_\nu .$$

Le matrici γ definite dalle (9), (15), (16) soddisfano le relazioni:

$$\gamma_\mu \gamma_\nu + \gamma_\nu \gamma_\mu = 2 g_{\mu\nu} \qquad \gamma_5 = \gamma_0 \gamma_1 \gamma_2 \gamma_3$$

$$g = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

e fornsicano quindi una realizzazione delle matrici di Dirac (si osservi che la particolare realizzazione ottenuta dipende dalla scelta della base $\hat{y}$ fatta nella (5)).

Il risultato più significativo dell'analisi precedente è il ruolo privilegiato delle correnti vettoriali (V) e vettoriali-assiali (A): le (14.1)-(14.2) indicano infatti che uno dei due tipi di spinori di Dirac (e = 1) ammette soltanto la costruzione delle forme V, A. L'intervento di particelle di questo tipo (potremmo orientativamente pensare ai leptoni) in una interazione debole a quattro fermioni condurrebbe quindi necessariamente ad hamiltoniane di tipo V, A.

La possibilità di correlare il ruolo privilegiato delle correnti V, A con proprietà "geometriche" dello spazio tempo appare dunque come una tipica novità di una descrizione basata su una geometria di Galois.

II. 6. - In quest'ultimo paragrafo raccoglieremo alcune osservazioni, parzialmente eterogenee, e che non svilupperemo in dettaglio, per ragioni di tempo.

Dal momento che il prodotto dell'inversione spaziale P per l'inversione temporale T ha immagine in L(4, p), ogni volta che venga precisata la rappresentazione di P risulta determinata quella di T e viceversa. In particolare, essendo il rappresentativo di PT lineare per costruzione, se P è rappresentato linearmente (o antilinearmente), altrettanto deve essere per il rappresentativo di T. Nel paragrafo precedente si è scelta una rappresentazione lineare, (γ_0), di P; risulta allora determinata la rappresentazione lineare τ di T:

$$\begin{cases} \tau = \chi \gamma_5 \gamma_0 , & \chi \chi^* = -1 , \quad \text{se } e = 0 , \\ \tau = \chi \gamma_0 , & \chi \chi^* = -1 , \quad \text{se } e = 1 . \end{cases}$$

Il carattere di linearità di τ e la sua forma esplicita (almeno nel caso e = 0) suggeriscono che T corrisponda, nel caso classico, al prodotto dell'inversione temporale per la coniugazione di carica. Invero si verifica facilmente che l'operazione PT trasforma le cinque correnti discusse nel precedente paragrafo in modo identico alla operazione CPT del caso classico.

Se, nel paragrafo precedente, avessimo rinunziato (come nel rif. (3)) a rappresentare linearmente P ed avessimo adottato una rappresentazione "alla Wigner" (antilineare) di T^* la coniugazione di carica sarebbe apparsa inclusa in P. In tal caso avremmo naturalmente potuto rinunziare ad introdurre spinori a quattro componenti, giacchè un rappresentativo antilineare di P su spinori a due

componenti è ovviamente possibile (questa è la possibilità particolarmente sviluppata nel rif. (3)).

Si può verificare che il ruolo privilegiato delle correnti V, A permane anche se P è rappresentato antilinearmente. Se, come di consueto, si associa la nozione di carica ad una trasformazione di gauge allora la quantizzazione della carica è conseguenza della struttura dei campi di Galois su cui abbiamo basato la nostra descrizione degli stati fisici (si veda il paragrafo II. 3).

Riferendosi ai campi spinoriali introdotti nel paragrafo II. 4, ogni cambiamento di fase di $\psi^{(e)}$ può essere formalmente introdotto trasformandolo con una rappresentazione di raggio (11) relativa ad $a = \mathbb{1}$:

$$\psi^{(e)} \longrightarrow S^{(e)}(\mathbb{1})\,\psi^{(e)} = \chi_{\mathbb{1}}\,\psi^{(e)}\,, \qquad \chi_{\mathbb{1}}\,\chi^{*}_{\mathbb{1}} = 1\,.$$

Sebbene ogni campo ψ sia definito a meno di un fattore di fase, la fase relativa di due campi può assumere significato: consideriamo ad esempio due campi che si trasformino rispettivamente con le rappresentazioni (omettiamo l'indice e, ora inessenziale):

$$S(a) \qquad \text{e} \qquad S_Q(a) = S^Q(\mathbb{1})\,S(a)\,, \qquad Q = 0, 1, \ldots, p^2-1\,.$$

Trasformando i campi relativi ψ e ψ_Q, corrispondentemente ad $a = 0$, si vede che ψ acquista un fattore di fase $\chi_{\mathbb{1}}$ mentre ψ_Q acquista un fattore di fase $\chi_{\mathbb{1}}^{Q+1}$. Si tratta dunque di una ordinaria trasformazione di gauge che suggerisce per Q l'interpretazione di carica.

Questo modo di introdurre la carica elettrica è particolarmente sottolineato nei rif. (2, 3) anche se in un diverso contesto (in particolare viene dichiarata, a nostro parere ingiustificatamente, la impossibilità di introdurre la nozione di carica per spinori a quattro componenti).

Un'altro argomento che può essere naturalmente sollevato è quello del gruppo di Poincarè. Vogliamo qui soltanto ricordare che nascono alcuni problemi inconsueti per la rappresentazione della parte abeliana del gruppo. Queste difficoltà sono legate alla impossibilità di "funzione esponenziale" sui campi finiti, o, in altre parole, alla ovvia impossibilità di un'onda piana infinitamente estesa in una geometria finita.

Infine vogliamo ricordare che la scelta, semi-obbligata, di rappresentazioni su campi finiti (paragrafo II. 3) apre il problema di studiare quale struttura concettuale di una meccanica quantistica sia possibile su tali campi. La impossibilità di trasferire inalterata la struttura consueta basata sulle proprietà dei reticoli delle proporzioni è stata recentemente discussa[13].

RIFERIMENTI. -

(1) - G. Jarnefelt, Ann. Acad. Sci. Fennicae A. I., No. 96 (1951); P. Kustaanheimo, Publ. Astron. Obs. Helsinki, No. 32 (1949); No. 34 (1952); No. 52 (1957); No. 55 (1957).

(2) - H. R. Coish, Phys. Rev. 114, 383 (1959).

(3) - I. S. Shapiro, Nuclear Phys. 21, 474 (1960).

(4) - V. G. Kadyshevskii, Soviet Phys. -Dokladi 6, 36 (1961).

(5) - H. Joos, J. Math. Phys. 5, 155 (1964).

(6) - Y. Ahmavaara, J. Math. Phys. 6, 87 (1965); 6, 220 (1965); 7, 197 (1966); 7, 201 (1966).

(7) - E. G. Beltrametti and A. A. Blasi, J. Math. Phys. 9, 1027 (1968); Nuovo Cimento 55A, 301 (1968).

(8) - E. G. Beltrametti and A. A. Blasi, Rend. Accad. Naz. Lincei (Cl. Sci. Fis. Mat. Natur.) 46, 184 (1969).

(9) - Vedi, ad esempio: L. Dickson, Linear groups (New York, 1958).

(10) - R. Steinberg, Can. J. Math. 3, 225 (1951).

(11) - Vedi, ad esempio: C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras (New York, 1962).

(12) - Vedi, ad esempio: M. Hamermesh, Group theory (Reading, 1962), Chap. 12.

(13) - J. P. Eckmann and P. C. Zabey, Helv. Phys. Acta 42, 420 (1969).